UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA,
ALEXANDRIA DIVISION

Project Honey Pot, a dba of Unspam Technologies, Inc.; and John Doe, on behalf of himself and all others similarly situated, Plaintiffs, v. Andrey Chernuk; Boris Livshits; St. Kitts-Nevis-Anguilla National Bank Limited; ZAO Raiffeisenbank; DnB Nord Banka; Bank Standard Commercial Bank Closed Joint-Stock Company; Azerigazbank; and Rietumu Bank; Defendants.	)	No. 1:11 CV 15 LMB/JFA

PLAINTIFFS' SECOND AMENDED COMPLAINT FOR VIOLATIONS OF THE FEDERAL FALSE MARKING ACT; FEDERAL RICO ACT; FEDERAL CAN-SPAM ACT; THE VIRGINIA COMPUTER CRIMES ACT; CONSPIRACY; NEGLIGENCE; NEGLIGENT ENABLEMENT; NEGLIGENT HIRING & RETENTION & UNJUST ENRICHMENT

1. Cyber crime is a global problem of epidemic proportions. Using vast networks of hijacked computers, counterfeiters, thieves and hi-tech snake-oil salesmen now have instant access to a global marketplace. No longer relegated to dark alleys, illegal and dangerous products are being advertised via spam emails, other forms of unsolicited mass communications, and even through paid online advertising, and are now only a mouse click away from every Internet user in the world. Cyber criminals do not even need a product to sell to make money.

Identity thieves, extortionists and phishers have opened Internet storefronts, and unwitting victims fall prey to them every day without ever leaving their living rooms.

2. Children and young adults are too often victimized by cyber criminals, who offer them easy access to illicit drugs, addictive drugs, gambling websites, pornography, fake IDs, spyware disguised as computer games or anti-virus software, and a host of other temptations. The elderly, the poor and the un- and under-insured are also being targeted by cyber criminals operating fake online pharmacies that are willing and able to ship cheap, counterfeit drugs to anyone with a credit card, no prescription required.

3. In addition to posing as legitimate online merchants, cyber criminals also commit crimes posing as fraudulent consumers, using stolen credit cards or other valuable tokens to purchase goods online or to steal money from hacked bank accounts. Unlike non-cyber criminals who are severely constrained by time and space, cyber criminals need only find an online process they can monetize, and then watch their profits roll in as they implement that process across the Internet and across the globe.

4. To commit their crimes, cyber criminals have formed complex organizations that are masterfully designed to avoid the technical defensive counter-measures that have been developed to date. At the strategic level, these counter-measures are little more than complex Turing tests[1] – capable of stopping machines that cannot learn, but incapable of stopping humans who quickly learn how to beat the test. Because humans are behind all acts of cyber crime, technology experts increasingly acknowledge that technical counter-measures,

[1] Introduced by Alan Turing in his 1950 paper *Computing Machinery and Intelligence*, a Turing test is a test of a machine's ability to exhibit intelligent (i.e., human-like) behavior. A human judge engages in a natural language conversation with one human and one machine, each of which tries to appear human. All participants are physically separated from one another. If the judge cannot reliably tell the machine from the human, the machine is said to have passed the test. The Turing test is considered an essential concept in the philosophy of artificial intelligence. For more information about Turing tests, see <http://en.wikipedia.org/wiki/Turing_test>.

operating alone, will never be able to effectively stop cyber crime. Because humans can find ways around the technical counter-measures faster than new counter-measures can be implemented, the fight against cyber crime is now highly asymmetrical – increasingly larger resources must be spent on technical cyber security to simply maintain the status quo. Many experts privately acknowledge we are falling further behind every day, and some even admit that cyber criminals are winning the war.

5. Cyber crime threatens us in fundamental ways that are both acute and chronic. As cyber crime organizations grow and mature, they identify aspects of their criminal business models that are critical to their success, and seek to strengthen or diversify points of weakness. They steal most critical resources – such as botnet computers that are used to transmit spam, launch distributed denial of service attacks or engage in other forms of illegal mass communications. What they cannot steal, they are forced to buy. Like all businesses, they seek to purchase critical resources from consistent suppliers at a competitive price. One of the most critical resources cyber criminals need is anonymity. But anonymity is not enough. To succeed, criminals must act anonymously while simultaneously fooling their victims into thinking they are a legitimate business or customer seeking to conduct a lawful transaction. **Thus, cyber criminals highly value (and highly compensate) vendors who willingly provide anonymity under a veneer of legitimacy. To stop cyber crime, cyber criminals must be cut off from these conspiring vendors. Indeed, their dependence on such vendors is perhaps the Achille's Heel of all economic cyber crime.**

6. If left unchecked, cyber crime has a natural tendency to lure willing enablers deeper into the conspiracy. As cyber criminals share the proceeds of their criminal operations with critical service providers, their illegal profits naturally tend to further corrupt

these providers. As enablers become corrupted, those with police authority over them become corrupted as well. Even nation-states are falling victim to cyber crime and the international organized criminal gangs that are behind it. Government corruption, failed legal systems and safe haven rules that generate a substantial portion of a nation-state's GDP all contribute to the problem, and are all being exploited by cyber criminals.

7. Economic cyber crime networks are also uniting with non-economic cyber crime networks – including cyber terrorists and hostile nation-state military and covert operations. This unity is not theoretical. Both economic and non-economic criminal elements are now fighting an aggressive, asymmetrical war with the United States. It is common knowledge within the industry that cyber attacks on the nation's critical infrastructure are increasing in scope and sophistication, and our ability to stop these attacks using technical means is diminishing. Botnets sending spam can also probe computers that control critical industrial infrastructure – power plants, air traffic control systems, and water supplies. Keystroke loggers capturing online financial data can also steal corporate intellectual property and government secrets. Botnet owners acquiring either of these data sets will seek to monetize the information in any way possible. Without increased effort and luck, someday soon the world will stop in its tracks as we collectively watch millions of Americans killed or displaced in a matter of minutes by a major industrial disaster because a system control and data acquisition (SCADA) device used to control and monitor industrial systems was destroyed in a cyber attack. It is highly likely that those who seek to commit such atrocities in the United States will succeed either with funds directly derived from economic cyber crime or by relying on critical service providers that have been corrupted by economic cyber crime.

8. Fortunately, the solution to these drastic problems already exists. It is the written law and enforcement measures that give teeth to these laws. Nearly every act of cyber crime violates numerous laws across nearly every jurisdiction in the world. Cyber crime thrives today not because we have failed to write laws properly, but because we are not systematically and cost-effectively applying the laws already on the books.

9. This lawsuit seeks to use well-established, existing laws to hold a cyber crime ring accountable for its illegal online pharmacy activity. This conspiracy includes at its center a small handful of financial institutions that are providing critical enabling banking services. The existing laws this lawsuit invokes include Federal RICO, the Federal False Marking Act, and the Federal CAN Spam Act, as well as common law conspiracy, negligence, and unjust enrichment.

* * *

10. Cyber crime encompasses a variety of illegal online activities, but spam is perhaps the most publicly visible sign of cyber crime, and thus provides an extremely effective window into the world of cyber crime. We cannot win the war on cyber crime without attacking the assault of spam that confronts us every day. A long list of laws already prohibits spam. Perhaps the most elegant is the centuries old common law of trespass to chattels, which one judge in this District suggested fit the spam problem like "a hand in glove." Notwithstanding that suggestion, a flurry of state and federal statutes have been passed over the last decade in an attempt to stop spam (or at least slow its growth) without unduly burdening "ham" (legitimate email). The culmination of this legislative activity was the Federal CAN-SPAM Act of 2003 (15 U.S.C. § 7701 et seq.).

11. CAN-SPAM, it was hoped, would help stop spam by clarifying the rules that bulk emailers were supposed to follow. The reality is that legitimate emailers generally complied with CAN-SPAM long before it was enacted, or at least complied to the degree that the identity of someone who accepted responsibility for the mailing could be found on the face of the message itself. Spam is different. On its face, spam never identifies anyone willing to accept responsibility for the mailing. The reason is simple – spam violates the most basic standards of good conduct. Once identified, spammers cannot defend their "business" practices to anyone, let alone to an upstream webhost, email service provider or judicial fact finder.

12. CAN Spam is hardly the only civil law that can be used to attack cyber crime. Other federal laws such as RICO, as well as tort law, contract law, and a host of state and federal statutes exist that provide powerful civil remedies to victims of all shapes and sizes.

13. If there were ever any doubt, today it is clear that the key to stopping cyber crime is identifying those responsible for it, their assets and their enablers, and getting that information into the hands of those willing and able to do something about it.

14. Discovering a cyber criminal's identity is not simple, but it is not impossible either. For example, spammers and those conspiring with them are relatively simple to identify if you know where to look. Plaintiff Project Honey Pot starts where most cyber crime begins – with the illegal harvesting of email addresses from websites. Illegal harvesting makes life on the Internet difficult for the rest of us because posting email addresses on a website is a convenient way to facilitate communications between visitors to a website and the owners of the website. Owners of websites who want to display email addresses can obtain some protection

from harvesters by installing a honey pot from Project Honey Pot on their website, and displaying this Project Honey Pot logo on their website:[2]

The logo serves as a warning to harvesters that all of the email addresses displayed anywhere on the website are protected by Project Honey Pot and deters harvesters by putting them at legal risk if they spam any addresses harvested from the website. Lawsuits of this kind are another effective way of deterring harvesters and the spammers who buy their harvested email lists.

15. Domain name owners who want to protect their email system from spam can obtain some protection by donating an MX record to Project Honey Pot, and then publicly disclosing the fact of their donation (but they should not disclose the specific MX record donated, as spammers will simply avoid this MX record and continue to send spam to MX records not donated to PHP). By publicly disclosing their affiliation with Project Honey Pot, PHP members warn spammers that their domain names are protected by Project Honey Pot.

Project Honey Pot, a dba of Unspam Technologies, Inc.

16. Project Honey Pot (www.projecthoneypot.org) (or "PHP") is a distributed network of spam-tracking honey pots. The Project allows spammers, phishers, and other e-criminals to be tracked throughout their entire "spam life cycle." On information and belief, Project Honey Pot was the first distributed e-mail harvesting research effort linking those that gather e-mail addresses by scraping websites with those that send unsolicited and frequently

[2] The website for the logo can be found at http://www.projecthoneypot.org/how_to_avoid_spambots_5.php.

fraudulent messages. Tens of thousands of users from at least 100 countries actively participate in Project Honey Pot's effort to track criminals who break the law via email. Project Honey Pot was created by Unspam Technologies, Inc (www.unspam.com) – an anti-spam company with the singular mission of helping design and enforce effective anti-spam laws. Unspam Technologies, Inc. is a Delaware corporation with its principal place of business at 5278 Pinemont Drive Suite A-135, Murray, Utah 84123.

17. Project Honey Pot receives MX record donations from the owners of Internet domain names. Through those donations, email messages addressed to any username hosted at a donated domain name are directed to email servers owned and maintained by Project Honey Pot, and those email messages are then processed by and stored by PHP on computer equipment, including computer equipment located in Arlington, Virginia. Project Honey Pot also makes available to Internet website owners email address honey pots that can be installed on their webpages. When a harvester visits those webpages looking for email addresses to steal, the harvester is handed a unique email address hosted within Project Honey Pot's distributed network of donated MX records. The harvester's IP address, the date and time of the visit and other characteristics of the harvester are recorded by Project Honey Pot and maintained for analysis and tracking. When a spam message is received thereafter at the unique email address, Project Honey Pot can tie the spam message (and the spammer) to the harvester that was given that email address.

18. Project Honey Pot is currently monitoring over 54 million honey pot addresses for annoying spam and dangerous phishing messages. Since Project Honey Pot first began monitoring spam, spammers have transmitted well over 1 billion spam messages to tens of thousands of unique email addresses belonging to PHP members who have donated an MX

record to, and are receiving anti-spam protection from, Project Honey Pot. All of these email addresses were illegally harvested by the spammer (or a co-conspirator) from a website hosting a PHP honey pot, or were the subject of dictionary spam attacks that indiscriminately targeted random usernames hosted within Internet domain names that have donated an MX record to, and are receiving anti-spam protection from, Project Honey Pot.

19. Since it started collecting data in 2004, Project Honey Pot has identified over 80 million spam servers, over 96 thousand harvesters, over 14 million dictionary attackers, and since April 2007, has identified over 348 thousand comment spam server IP addresses.

20. Every spam message transmitted to a Project Honey Pot honey pot email address harms Project Honey Pot. Each spam message is received by a mail server controlled by and paid for by Project Honey Pot, which then must process, store and analyze the message to help protect the website owners who have installed honey pots on their webpages from harvesters, and to protect the domain name owners who have donated MX records from spam attacks. Moreover, the spam received directly by Project Honey Pot is only a small fraction of the total spam received by the domain name owners protected by Project Honey Pot. Project Honey Pot estimates that 125,000 spam messages are transmitted globally for every single spam message received by one of its honey pot email addresses. With over 1 billion spam messages in Project Honey Pot's inbox, this equates to 125 ***trillion*** spam messages transmitted globally since 2004 by all spammers, and roughly equates to hundreds of millions of spam messages transmitted globally by the Defendants in this case alone.

Plaintiff John Doe

21. Plaintiff John Doe is a resident of Arlington, Virginia. John Doe's name is listed as an alias because he is concerned about his personal safety arising from this lawsuit.

The allegations in this Complaint are being leveled against an international criminal enterprise, including corporate actors with vast resources available to them and individual actors who are, or have at one time been, present in the United States, and presumably have the ability to re-enter the United States or have the ability to coordinate with co-conspirators located within the United States. In addition, it is very likely that other individuals and corporations not yet identified will be added to this lawsuit or could face other legal consequences based on information developed by this lawsuit. Without knowing the identities of all the defendants or potential defendants to this lawsuit, John Doe is unwilling to identify himself publicly at this time.

22. In October 2007, John Doe attempted to purchase a well-known brand name prescription blood pressure medication at an online website doing business under the trade name "Canadian Pharmacy." Although John Doe had a lawful prescription for this medication, he was not asked by the website to provide any prescription information or the name of his prescribing doctor. He made payment for his purchase using a Visa debit card connected to his checking account. The card number included a unique identification number that the merchant could use to identify John Doe's bank. John Doe also provided to the Defendants his home address as the delivery point for the medication. John Doe learned of the website either by clicking on a search engine result, a paid ad displayed on a website, or a spam email he received at a proprietary email address within an Internet domain name he owns and uses to conduct his business. The Canadian Pharmacy website also displayed the telephone number 210-787-1711 as a contact number for the pharmacy. According to an archival capture of the website taken by the Wayback Machine in October 2007, the pharmacy website visited by John Doe claimed it was licensed by the College of Pharmacists of British Columbia, that its physicians were U.S.

licensed and board certified, and that its pharmacies were U.S. licensed. On information and belief, none of these statements by the Defendants was true.

23. Following John Doe's attempted purchase, his debit card was charged the amount displayed on the website at the time he completed his purchase. According to the transaction information included on his bank statement (all of which information is provided by the merchant and the merchant's bank), the merchant's name was reported to be "IP-RXOEM.COM," and an apparent US-based telephone number was listed as "6074280039." John Doe subsequently received an email notice confirming his purchase. That notice was sent to the email address he provided in the online order form. That notice also stated his medication would arrive via US Postal Service in 10-15 days. The confirming email also provided a tracking number he was told could be used at the USPS website to track his package en route. When he entered the tracking number over several days, however, the USPS website reported it had no record of this item.

24. When no medication arrived after several weeks, John Doe then attempted to contact the online pharmacy at the telephone number listed on the website. On most occasions, his call was never answered, and when the call was answered, a voice recording played in English asking him to leave a message. He left messages which were never returned. John Doe also tried contacting the online pharmacy by replying to the confirmation email and by sending a web-based message through the "contact us" link he found on the website. He never received a reply to any of his electronic messages.

25. In December 2007, John Doe notified his bank of the fraudulent charge and asked to have the transaction reversed. The funds charged to his account were then credited to his account, and his card number was then changed by his bank to prevent the card from being

charged again by the merchant. However, John Doe continues to use his checking account with that bank and continues to use the same email address he provided the online pharmacy. By closing the card he used in his purchase, John Doe's bank has incurred costs associated with closing and reissuing him a new card. In some cases, issuing banks are recouping these costs by increasing costs and fees to consumers.

26. John Doe's email address is tied to a proprietary domain name he owns and uses in connection with his business. It would not be simple or cost free for him to change the email address or his proprietary domain name. That email address has received a very large volume of spam email messages in the months since he submitted his online order. Many of these spam messages are advertising online pharmacies, and many also contain information about John Doe that indicates the message was sent by someone who has access to the information he submitted in attempting his purchase. For example, some of the messages contain a personal greeting matching his first and last name (which are not apparent from his email address alone); some emails identify his city and zip code, and some even offer to refill his original order. In addition to these messages, John Doe also receives a large volume of spam messages that cannot on their face be tied to his attempted purchase but that, on information and belief, are being sent by the Defendants. On information and belief, the Defendants do not honor remove requests to stop transmitting these advertisements, and requests to be removed simply encourage more spam because they confirm that the email address is being monitored by a real human.

27. John Doe has attempted, through counsel, to determine the identity of the merchant bank that provided charging privileges to the online pharmacy merchant, and the identity of the merchant, by asking John Doe's bank to provide information available to it about

the underlying transaction. John Doe's bank has offered to produce this information if subpoenaed, but has declined to voluntarily produce the information. On information and belief, the merchant bank that initiated John Doe's transaction is one of the banks specifically named herein, or is another bank conspiring with the Pharmacy Defendants. On information and belief, the Pharmacy Defendants include the merchant that initiated John Doe's transaction.

The Pharmacy Defendants

28. Defendant Andrey Chernuk's residence and citizenship are unknown to the Plaintiffs. On information and belief, Mr. Chernuk has used at least two private mail box services in Florida to receive mail – one at 1901 60th Place E, Box L4385, Bradenton, FL 34203, and the other at 1455 Tallevast Road, Box L1128, Sarasota, FL 34243.

29. Defendant Boris Livshits' residence and citizenship are unknown to the Plaintiffs. On information and belief, Mr. Livshits was residing for a period of time relevant to this complaint at an apartment building in Brooklyn, New York. He has also used at least two private mail box services in Florida to receive mail – one at 2950 NE 32nd Avenue, Box A-1374, Fort Lauderdale, FL 33308-7219; and the other at 1903 60th Place E, Box M4283, Bradenton, FL 34203-5036.

30. On information and belief, Defendants Chernuk and Livshits are conspiring with other persons and entities to operate an illegal online pharmacy business under a number of fictitious pharmacy trade names. The identities of these unnamed co-conspirators are not yet known to the Plaintiffs, but should be discoverable from records maintained by the Defendants or by third parties subject to subpoena in this case. Hereinafter, the term "Pharmacy Defendants" is used to refer collectively to Defendants Chernuk and Livshits and the as-yet unnamed persons and entities with whom they are conspiring.

The Merchant Bank Defendants

31. The Pharmacy Defendants have used a number of merchant accounts at a handful of financial institutions throughout the world to convert the debit and credit card information they obtained from consumers into cash. Each of the financial institutions identified below has provided merchant account card processing services to the Pharmacy Defendants, and is a merchant bank participating in the Visa network.

32. Defendant St. Kitts-Nevis-Anguilla National Bank Limited (hereinafter SKNANB) is a public limited company registered in St. Kitts & Nevis, and headquartered at PO Box 343, Central Street, Basseterre, St. Kitts 00265, West Indies.

33. Defendant ZAO Raiffeisenbank (hereinafter Raiffeisenbank) is a wholly owned subsidiary of Raiffeisen Bank International AG, operating in Russia since 1996, and is supervised by the Bank of Russia. In or around February 2006, Raiffeisenbank merged with OAO Impexbank, which had originally been founded in 1993, under General License No. 2291, issued by the Bank of Russia. The Pharmacy Defendants have used merchant accounts with OAO Impexbank prior to the merger, and with Raiffeisenbank post-merger.

34. Defendant DnB Nord Banka (hereinafter Nord) is a European bank group headquartered in Copenhagen, Denmark, with offices at Skanstes iela 12, Riga, Latvia. Nord is a wholly owned subsidiary of DnB Nor Bank ASA, a Norwegian public limited company.

35. Defendant Bank Standard Commercial Bank Closed Joint-Stock Company (hereinafter Bank Standard) is an Azerbaijan joint stock company, headquartered at 4, Azerbaijan Avenue, Baku, AZ1005, Azerbaijan. Established in 1995, Bank Standard is the largest private bank in Azerbaijan.

36. Defendant Azerigazbank (hereinafter AGBank) is an Azerbaijan open investment company, headquartered at 16, Landau str., Baku, Azerbaijan.

37. Defendant Rietumu Bank (hereinafter Rietumu) is a Latvian joint stock company, headquartered at Veseta 7, Riga LV-1013, Latvia.

38. On information and belief, the banks specifically named above are conspiring with other persons and entities to provide merchant account card processing services to the Pharmacy Defendants. These other persons and entities include merchant account brokers, independent sales organizations and processors, and Internet Payment Service Providers (which, according to Visa International's Operating Regulations, are online entities that contract with a merchant bank to provide payments services to a merchant). The identities of these unnamed co-conspirators are not yet known to the Plaintiffs, but should be discoverable from records maintained by the Defendants or by third parties subject to subpoena in this case.

39. On information and belief, additional not-yet-identified merchant banks have provided or are providing merchant account card processing services to the Pharmacy Defendants. Hereinafter, the term "Merchant Bank Defendants" is used to refer collectively to these not-yet-identified merchant banks, as well as the banks specifically named above and the not-yet-identified third parties conspiring with them.

The Defendants' Illegal Scheme

40. On information and belief, Pharmacy Defendants Andrey Chernuk and Boris Livshits are the owners and operators of an illegal online pharmacy business. This pharmacy operates under a number of trade names, including the trade name "Toronto Pharmacy." Toronto Pharmacy operates through a host of domain names that all present a similar webpage layout and design to the viewer, as depicted here (a larger version is included as Exhibit A):

41. From at least 2006 to the present, Toronto Pharmacy has used at least 170 domain names to host its pharmacy business websites or to facilitate ancillary services necessary to its operations.

42. Between 2006 and the present, websites operating under the Toronto Pharmacy trade name have been advertised in thousands of spam messages transmitted to email addresses managed by Project Honey Pot. Each of these spam emails advertised one or more of Toronto Pharmacy's 170 domain names, and each website could be visited by a viewer of the email by simply clicking on the link in the email message. A true and correct copy of a sample of the Toronto Pharmacy spam messages is attached as Exhibit B. Some spam emails consisted of images of well-known patented brand name drugs with a hyperlink embedded in the image leading to a Toronto Pharmacy website. Other emails consisted of text and a hyperlink leading to a Toronto Pharmacy website. Sometimes the text in the email was arrayed in a multi-column table format. On information and belief, spam messages are arrayed across table columns to make it more difficult for spam filters to parse and thus block the message. On information and belief, each of the Toronto Pharmacy spam messages was transmitted to Project Honey Pot through a compromised "botnet" computer, and thus originated from an IP address fraudulently

accessed by the Defendants, and each spam message contained a false or fraudulent email address in the from line.

43. On information and belief, in addition to doing business under the trade name Toronto Pharmacy, Defendants Livshits and Chernuk also operate their illegal online pharmacy under (or conspire with others operating under) a host of other trade names, including but not limited to: Canadian Health & Care Mall, Canadian Meds, Canadian Pharmacy, ED Med Chest, ED Med Choice, ED Pills, eScripts, European Meds, Exclusive Generics, Express Drug Mart, Finest Rx, International Legal Rx, Medic Suite, MyCanadianPharmacy, Patriot Prescriptions, Pharmacy Express, Pharma Shop, Premier Pharmacy, RxNet, RxOrdersFast, RxPharmaDeals, RxPharmaDrugs, US Drugs, US Healthcare, US Pharmacy, VIP Pharmacy, and World Pharmacy.

44. Collectively, these pharmacy trade names are all being hosted on thousands of domain names advertised through hyperlinks in hundreds of thousands of spam messages that have been transmitted to Project Honey Pot, and are being used to lure consumers in the United States to purchase counterfeit medications through false and misleading representations about the online pharmacy and the medications being sold.

45. Beginning in 2004 and continuing to the present, PHP has captured vast amounts of computer data relating to these online pharmacies, including information concerning: the harvesters used to collect email addresses to which spam advertising these online pharmacies was transmitted to PHP, spam messages advertising these online pharmacies transmitted to PHP, source code of the online pharmacy web pages, technical information underlying these web pages (including A, MX and DNS records, WhoIs records, and IP block records for the thousands of domain names and/or IP addresses connected to these online pharmacies).

46. The connections between and among these trade names are numerous and persistent, and have recurring connections to the named Defendants. For example, the telephone number displayed on the "Canadian Pharmacy" website that Plaintiff John Doe visited (210-787-1711) also appears on other pharmacy websites operating under different trade names, including "European Meds" and "Canadian Meds World." True and correct copies of these websites, showing the same telephone number, are attached as Exhibit C. The European Meds pharmacy website was, in turn, advertised on adult content websites through banner ads presented on the side of those adult content websites. Those adult websites, in turn, listed Defendant Livshits' residence in Brooklyn, New York as a contact address for the adult content websites.

47. The Defendants sell counterfeit prescription medicine (including controlled substances) but advertise their products as brand name, patented drugs that enjoy FDA approval and that are lawfully sold in the United States. The drugs actually shipped to consumers by the Defendants, however, are not FDA approved, are not patented drugs, and may not be lawfully sold in the United States. The Defendants also do not require consumers to provide a lawfully acquired prescription from a doctor to buy prescription drugs. Nor are the Defendants licensed by any state in the United States to sell prescription drugs to consumers in that state, nor are they licensed by the U.S. Drug Enforcement Agency to sell controlled substances in the United States.

48. The Pharmacy Defendants have the ability to charge Visa debit and credit cards to collect payment for the medications they sell, via merchant accounts established with the Merchant Bank Defendants, all of whom are members of the Visa network. Without a merchant account at a merchant bank, the Pharmacy Defendants could not offer the convenience to consumers of being able to pay by credit card, and would be forced to use an inferior payment

collection method, such as asking consumers to mail a check, cash or a money order to a physical address, or to wire funds to a bank account through a money transfer agent.

49. In addition to the convenience of collecting payment by credit card, the Pharmacy Defendants' access to the Visa network also conveys an image of legitimacy to their websites, because consumers believe merchants must meet certain standards in order to qualify for credit card merchant charging privileges.

50. On information and belief, Defendants are collecting credit and debit card information from consumers through unencrypted Internet connections. Visa, like all other major card networks, requires online merchants to collect payment information over the Internet through an encrypted connection to prevent third parties from seeing the card data in plaintext. Defendants are not using secure connections in all instances and are thus compromising the integrity of consumer card information being passed in plaintext.

51. In addition to exploiting the Visa brand, the Defendants' pharmacy websites also falsely claim their pharmacy is approved or affiliated with a number of authentic (or purportedly authentic) third party trust organizations, including but not limited to: the American Drug Administration (which is sometimes displayed on the pharmacy websites under the logo for the United States Food and Drug Administration), Better Business Bureau, CIPA, IMPAC, Pharmacy Checker, Square Trade, and Verisign.

52. In addition, the Defendants typically claim some connection to Canada – either by posting a Canadian physical address on their website that purports to be their headquarters or brick and mortar pharmacy location, or by claiming to be licensed by a Canadian legal authority. In reality, the Defendants have no real connection to the physical addresses and do not have any license or other authorization from Canadian authorities to operate a pharmacy

online. Even if they did, a Canadian physical address or license would not authorize the Defendants to sell medications to United States consumers, and certainly would not authorize them to sell counterfeit medications, without a prescription and without a pharmacy license from the relevant state board of pharmacy, or to sell controlled substances without a license from the United States Drug Enforcement Agency.

53. The Pharmacy Defendants are using merchant accounts to charge consumer debit and credit cards of United States residents and to collect funds through one or more of the Merchant Bank Defendants. On information and belief, the Pharmacy Defendants and Merchant Bank Defendants are also conspiring with or through merchant account brokers, independent sales organizations and processors, including Internet Payment Service Providers (which, according to Visa International's Operating Regulations, are online entities that contract with a merchant bank to provide payments services to a merchant). The complete organizational structure of the conspiracy is not yet fully known to the Plaintiffs, but will be discoverable from information to be produced by the Defendants, or by Visa International, Visa USA, other card network operators, or other third parties subject to subpoena in this case.

54. In addition to their illegal pharmacy operations, the Pharmacy Defendants also have interests in other online businesses, including adult-content websites, fake luxury goods websites, and fake anti-virus software and computer software download websites. On information and belief, the Pharmacy Defendants are also processing non-pharmacy debit and credit card sales through the Merchant Bank Defendants. The full extent and nature of their related non-pharmacy online businesses are not yet known to the Plaintiffs.

55. On information and belief, in addition to operating illegal or fraudulent merchant websites, the Pharmacy Defendants are also using stolen credit cards or credit cards

obtained through their merchant operations to steal services necessary to their online pharmacy and non-pharmacy operations and to steal consumer goods from legitimate merchants within the United States. Cards used for this sort of secondary fraud are typically closed once the fraudulent charge is discovered, and new physical cards and card numbers are issued by the bank to the cardholder. The cost of closing and reissuing cards and numbers is typically borne by the issuing bank in the first instance, but is ultimately passed onto accountholders in increased fees and costs. Cards are also routinely closed (and costs incurred) even in the absence of secondary fraud on the card, whenever a consumer alerts the issuing bank that medication was purchased online under suspicious circumstances, as happened when John Doe alerted his bank about his attempted purchase.

56. On information and belief, the Defendants are also using the fact that some members of the Class purchased certain types of medication (such as controlled substances) to extort money from the Class members by contacting the Class member by email or telephone, while posing as a law enforcement authority. The FDA has issued a warning to the public concerning this ongoing extortion threat.[3] The Defendants extort money from susceptible Class members by falsely and without authority threatening to investigate or arrest the Class member for purchasing controlled substances. Class members who succumb to this extortion attempt face further extortion threats. On information and belief, some Class members have lost tens of thousands of dollars from this extortion scheme.

57. On information and belief, the Defendants are also using information obtained from the Class members to transmit phishing emails to the Class members, in which the emails purport to be from the member's bank. This type of phish email is commonly referred to

[3] http://www.fda.gov/ICECI/CriminalInvestigations/ucm239309.htm.

as "spear phishing" because the phisher can tailor the email to the specific bank used by the member. Spear phishing allows a phisher to expose to law enforcement a much smaller fingerprint for the same pay-out because his emails are targeted only to those persons known to bank at a particular financial institution. These emails ask the member to log onto a fake bank website or download a virus program that allows the Defendants to collect the Class member's online banking credentials. This in turn allows the Defendants to access the member's bank account via the Internet and steal funds from the account or engage in other illegal conduct using the information. Individuals who fall victim to these phishing attacks can be personally liable for the resulting losses, particularly those who provide the phisher with a business banking account, because business banking accounts do not enjoy the same anti-fraud protections that apply to individual bank accounts under traditional banking laws. In cases where the account holder is held harmless, the bank reimburses the accountholder and assumes the loss. In either case, a member of the proposed Class of consumers and banks bears the loss for funds stolen by the Defendants through phishing and spear phishing.

CLASS ACTION ALLEGATIONS

58. The Class consists of all individuals in the United States who used a debit or credit card to purchase or attempt to purchase medications online at websites controlled by the Pharmacy Defendants, and their card issuing banks. The Class can ultimately be determined easily by reference to credit card transaction records that will be found within the control of Visa International, Visa USA, and/or the Merchant Bank Defendants determined to have provided merchant accounts to the Pharmacy Defendants.

59. The Class is so numerous that joinder of all members individually is impracticable. Class members are located throughout the United States. On information and

belief, the Pharmacy Defendants have collected hundreds of millions of dollars from American consumers over several years. Because the typical transaction is approximately $200, it is reasonable to believe the defendants processed millions of transactions, and that hundreds of thousands (if not millions) of unique class members are involved.

60. Plaintiff John Doe is an adequate class representative of the Class and his claims are typical of those of the Class. There are no issues or defenses unique to John Doe, and John Doe has no conflicts with the members of the Class.

61. There are questions of law and fact that are common to the Class and that predominate over any issues affecting only individual members. Common questions of fact include: the sources of medications supplied by the Pharmacy Defendants and whether those sources were lawful suppliers of the brand name medications advertised by the Pharmacy Defendants or were unlawful suppliers of counterfeit medications; the false nature of the statements, photographs/graphics and other representations appearing on the websites and in other advertising materials distributed by the Pharmacy Defendants; whether the Pharmacy Defendants had any legal authority (via DEA licenses, state board of pharmacy licenses or other legal authorization) to dispense prescription drugs to consumers within the United States or any state within the United States; the Merchant Banks' knowledge of the illegal activity of the Pharmacy Defendants, as evidenced by the information provided by the Pharmacy Defendants (or gathered by the Merchant Banks) as part of the merchant application and review process, and as part of the daily operations of the merchant account, including the information obtained by the Merchant Banks through charge backs initiated by consumers who realized or suspected the medications they received were not what they were led to believe or were otherwise illegal, unsafe or ineffective. Common questions of law include whether the Defendants violated the

Federal False Marking Act and the Federal RICO Act, whether the Defendants entered into an unlawful conspiracy, and whether the Merchant Bank Defendants acted negligently in providing merchant account processing services to the Pharmacy Defendants, acted negligently in hiring and retaining third party merchant account brokers, independent sales organizations and processors, including Internet Payment Service Providers, and whether they were unjustly enriched by the illegal activities of the Pharmacy Defendants.

62. A class action is superior to other available methods for the fair and efficient adjudication of this controversy. The individual claims of the class members are too small to warrant their bringing individual actions. In addition, it would be extremely difficult for individual class members, acting alone, to obtain the technical and financial information needed to prosecute their claims. Not even Plaintiff John Doe, with the assistance of counsel, was able to obtain from his own bank the identity of the merchant bank and merchant account number that initiated the transaction charging his account. John Doe's experience is typical of that of the consumer members of the Class, with issuing banks demonstrating great reluctance to provide this information even to their accountholders. In addition, consumer Class members are unlikely to prosecute their claims because of concerns they may be subject to government investigations and criminal charges. Although the United States Government has indicated individual consumers purchasing non-controlled prescription medicines online in small quantities for personal use without a prescription will not be prosecuted, such actions are still technically against the law. Moreover, those consumer Class members who are most vulnerable to the Defendants' scheme are those who purchased or attempted to purchase controlled substances online without a prescription. It is illegal for consumers in the United States to attempt such purchases, and the federal government has not published a policy of non-prosecution with regard

to persons purchasing controlled substances online without a prescription. Class members buying controlled substances are also more likely to be suffering from debilitating physical pain, illness, and chemical addictions that render them less able to pursue their legal rights in the absence of action by the Class on their behalf. Thus, those members of the Class who need the most protection are those least likely to pursue individual action. To the best of John Doe's knowledge, there is no other action brought on behalf of the Class against the Defendants. It is desirable, therefore, for this litigation to proceed in this Court, which is already familiar with the background of this lawsuit. There should be no difficulties in the management of this action as a class action, since much of the information needed to identify the Class members will be discoverable through Visa USA or Visa International records, other card networks, other third parties subject to subpoena, or from the Merchant Bank Defendants or Pharmacy Defendants.

JURISDICTION AND VENUE

63. This action arises out of Defendants' violation of the Federal False Marking Act, the Federal RICO Act, and the Federal CAN-SPAM Act. The Court has subject matter jurisdiction of this action under these claims based on 28 U.S.C. § 1331, and supplemental jurisdiction over the state law claims under 28 U.S.C. § 1367.

64. Pursuant to 28 U.S.C. § 1391(b)(2), venue is proper in this judicial district. Plaintiff John Doe resides in this district and all of his actions in attempting to purchase medicine online were undertaken within this district. He provided a mailing address within the district to the defendants, and he paid using a debit card tied to a bank account located within the district, with a bank doing business within the district. In addition, a substantial part of the events or omissions giving rise to Plaintiff Project Honey Pot's claims, together with a substantial part of the property that is the subject of Plaintiff Project Honey Pot's claims, are situated in this judicial

district. For example, 886 PHP members self-report they are located in Virginia. PHP members have installed honey pots on 287 websites that are hosted on IP addresses located in Virginia, and these Virginia-based honey pots have distributed tens of thousands of email addresses to identified harvesters world-wide. In addition, a substantial portion of the computer equipment used by PHP to process and analyze the spam messages, collect the web pages and the technical information underlying the domain names and/or IP addresses connected to those web pages, is located in Arlington, Virginia.

65. In addition to John Doe's and PHP's substantial presence in Virginia, the Defendants also have substantial connections to Virginia and this district. For example, Defendants have harvested email addresses from computers located within Virginia and this district or from websites owned and controlled by PHP members located in Virginia, and have used compromised computers and/or IP addresses located in Virginia to transmit their spam messages to PHP and the Class. In addition, the online pharmacy web pages controlled by the Defendants were all generally visible to consumers surfing the web from within Virginia and the district, and medications were shipped to physical addresses in Virginia. While making their websites available to consumers within Virginia and this district, the Defendants have also taken specific technical evasive actions to avoid being detected by investigators located within Virginia and this district, including PHP. Specifically, the Defendants have systematically null routed and DDOS'ed[4] PHP's attempts to collect open source information about the Defendants' online

[4] "Null routing" occurs when a web server is programmed to simply not respond to a request for a webpage from a web browser, based on particular characteristics of that web browser. "DDOS" stands for distributed denial of service. A DDOS attack can occur in a number of ways, but in this case, the Defendants routinely directed a flood of junk transmissions (typically UDP traffic) toward the Virginia-based IP addresses tied to the computers being used by PHP to capture the Defendants' publicly-available online pharmacy websites, effectively slowing those computers to a crawl and making it more difficult for PHP to collect the open source data needed to make the connections between the various Internet identities used by the Defendants to hide the overall size, nature and scope of their illegal enterprise that is alleged in this Complaint.

pharmacy websites where those attempts originated from IP addresses located within Virginia. Thus, the Defendants have knowingly and intentionally engaged in a continuing pattern of business whereby they attempt to make their online pharmacy websites freely and easily accessible to consumers within Virginia and this district, but inaccessible to legal investigative efforts undertaken from within Virginia and this district.

66. The federal District Court for the Eastern District of Virginia has personal jurisdiction over Defendants based on the following facts: Defendants initiated emails from the this district, gained unauthorized access to computer servers located in this district, caused tortious injury in this district, shipped product into this district, collected funds from persons located within this district, conducted business in this district, or conspired with persons who engaged in these jurisdictionally significant acts.

COUNT I
Violation of the Federal False Marking Act (35 U.S.C. § 292)
By All Plaintiffs Against All Defendants

67. Plaintiffs Project Honey Pot and John Doe, on behalf of himself and the Class, repeat and re-allege the allegations in paragraphs 1 through 66 of this Complaint.

68. Defendants, without the consent of the patentees, have used in advertising in connection with counterfeit medications made, used, offered for sale, or sold within the United States, or imported into the United States, the name or imitation of the name of the patentees, or the like, with the intent of counterfeiting or imitating the mark of the patentees, or of deceiving the public and inducing them to believe that the counterfeit medications were made, offered for sale, sold, or imported into the United States by or with the consent of the patentees.

69. Defendants have used, in advertising in connection with counterfeit, unpatented medications, the brand names of patented medications for the purpose of deceiving the public.

70. As a result of the Defendants' false markings, Defendants should be fined $500 for every such offense. An offense occurred each time: (1) Project Honey Pot received a spam email message advertising the Defendants' pharmacy business; (2) each time John Doe or any member of the Class visited one of the Defendants' pharmacy websites and attempted to purchase medication; and (3) each time a spam email message advertising the Defendants' pharmacy business was transmitted into or within the United States. Pursuant to the False Marking Act, one-half of any assessed fine should go to the Plaintiffs, and the other half to the use of the United States.

COUNT II
Violation of the Federal RICO Act (18 U.S.C. § 1962(c) et seq.)
By All Plaintiffs against All Defendants

71. Plaintiffs Project Honey Pot and John Doe, on behalf of himself and the Class, repeat and re-allege the allegations in paragraphs 1 through 66 of this Complaint.

72. Defendants Chernuk, Livshits, the named Merchant Banks, and the unnamed Pharmacy and Merchant Bank Defendants are persons as defined in 18 U.S.C. § 1962(3).

73. The online pharmacy businesses operating under a variety of trade names including Toronto Pharmacy and the other trade names listed in paragraph 43, along with the domain names hosting the pharmacy websites (which would have appeared in the address bar of any person viewing the websites in a browser) or invoked as the name of the merchant in the credit card transaction information appearing in John Doe's card statement and the card statements of the Class members, are enterprises or an enterprise as defined in 18 U.S.C. § 1962(4) (hereinafter the "Pharmacy RICO Enterprises").

74. Chernuk, Livshits, other Pharmacy Defendants not yet identified, and the Merchant Bank Defendants participated in the conduct of the affairs of the Pharmacy RICO

Enterprises identified in the prior paragraph from at least 2006 through the present through a pattern of racketeering activity as that phrase is defined in 18 U.S.C. § 1961(5).

75. The Pharmacy RICO Enterprises share common owners and managers and performed the same business activities as described above. Each of the entities was an essential element in a common fraudulent enterprise whereby the online pharmacy businesses illegally and fraudulently sold counterfeit medications to consumers, obtained credit card information from consumers, converted those card numbers into funds through the Merchant Bank Defendants which funds were disbursed among the Defendants, and engaged in additional illegal racketeering activity.

76. With knowledge of the criminal conduct of the online pharmacy businesses, or with willful disregard thereof, the Merchant Bank Defendants, and each of them, provided the necessary merchant bank services to convert the consumer credit card information into cash. The Merchant Bank Defendants knew or willfully disregarded information showing the online pharmacy businesses were engaged in the illegal sale of counterfeit medications online through card not present transactions with US-based consumers. The information available to the Merchant Bank Defendants was voluminous. Visa's requirements for merchant banks require banks acquiring merchants to conduct a physical inspection of the business premises and to obtain a detailed business description for electronic commerce merchants. Each merchant must also be correctly coded by the merchant bank with a four digit Merchant Category Code (MCC). The MCC for pharmacy/drugstore is 5912. On information and belief, most (if not all) of the MCC's assigned to the Pharmacy Defendants' merchant accounts by the Merchant Bank Defendants were MCC 5912, corresponding with pharmacy/drugstore businesses. Thus, the Merchant Bank Defendants clearly knew the Pharmacy Defendants were in the business of

operating online pharmacies. Thus, they knew or should have known to inquire about government licensing, procurement sources, and shipping methods and locations, as well as customer-bases to ensure compliance with applicable laws and regulations. In addition, merchant banks are required by Visa to determine that a prospective merchant is financially responsible and that there is no significant derogatory background information about any of its principals, using information obtained through credit reports, personal and business financial statements, income tax returns and any other information lawfully available to the merchant bank. It is commonly understood by merchant banks in the credit card industry that pharmacy/drugstore merchants are "high risk" businesses, and thus require greater diligence on the part of the merchant bank to ensure the merchant is complying with Visa's merchant rules and regulations. Merchant banks are also required to implement anti-money laundering and anti-fraud policies and procedures (under US law and other nations' laws) that could and should have prevented the Pharmacy Defendants from becoming merchants. In addition, the Merchant Banks had access to information provided by the merchants as part of the application process, including the merchant's prior internet business history, prior credit card processing history, screenshots and domain names of the merchants' disclosed websites, public and non-public information about web traffic statistics tied to the disclosed websites claimed by the Pharmacy Defendants, and a wealth of related information that could be used to connect the merchants' disclosed domain names (and other information contained in their merchant applications) to more permanent Internet technical data points (such as the A, DNS and MX records, IP blocks, and hosting ASN's tied to the disclosed domain names, as well as registrar and registrant information). All this information can also be tracked over time to show historical changes with respect to both web page content and technical hosting information behind the domain names. In

addition, the merchant banks could have queried any number of reputational databases to determine whether the applicants had any historical connections to illegal online pharmacies, spam activity, email harvesting activity or other types of fraudulent or illegal Internet activity.

77. Even if the illegal nature of the Pharmacy Defendants' business had escaped detection at the merchant application stage, it could and should have been detected by the Merchant Bank Defendants shortly after opening the merchant account. Visa requires merchant banks to monitor merchant business activity and variations in that activity over time to detect abnormalities that constitute red flag warnings of potential fraud or illegal activity. The statistics tracked include, but are not limited to: gross sales volumes, average transaction amounts, number of transaction receipts, the time it takes to complete a transaction, and chargebacks. A chargeback is a credit card transaction that is reversed – typically because the customer is unsatisfied with the transaction for any number of reasons. Chargebacks, in particular, provide the merchant bank with a wealth of information about the details of the merchant's business, because the chargeback can include comments from the consumer explaining the reason for the chargeback. Thus, chargebacks are very likely to reveal information sufficient to put the merchant bank on notice of any number of red flags including: the medications being sold are counterfeit (for example, if a consumer complained "the pills arrived in a plastic baggy and looked like they'd been made in someone's basement"), harmful to the consumer ("I took one pill and it made my heart race/made me sick/ sent me to the hospital"), or were shipped across international borders in violation of customs laws or in a manner that suggests the shipper went to great lengths to hide the contents from customs authorities ("the pills were shipped from China and were wrapped in a Chinese language newspaper" or "the pills were hidden in the fake bottom of a jewelry box…is this illegal?"). On information and belief,

the Pharmacy Defendants' merchant accounts experienced chargebacks that would have included information raising these and other red flags with the Merchant Bank Defendants. Even without the information derived from chargeback analysis, the activity tracking should have revealed the Pharmacy Defendants were engaged in illegal and fraudulent business. New merchants must establish a baseline of activity, and that baseline must be consistent with the prior business history provided by the merchant applicant. A merchant that claims no prior business history should not produce high sales volumes upon the opening of the account, and a merchant who does produce high sales volumes should be able to provide a verifiable prior business history in its application to explain the high sales volumes it is immediately generating upon opening the account.

78. Once a fraudulent or illegal merchant is identified by the merchant bank, Visa's operating rules require the merchant bank to report the activity to the proper authorities within the Visa network, so that the merchant (and its principals) can be denied access to Visa services from any merchant bank. On information and belief, the Merchant Bank Defendants failed to properly report the Pharmacy Defendants to Visa, other card network operators, and other proper authorities.

79. For the reasons stated above, the Merchant Bank Defendants were on notice of and knew of the unlawful scheme being perpetrated by the Pharmacy Defendants as alleged herein, but participated in the scheme, and committed acts in furtherance of that scheme by continuing: (1) to process credit card transactions, (2) to open new merchant accounts for the Pharmacy Defendants; (3) to collect funds from transactions tied to merchant accounts controlled by the Pharmacy Defendants, (4) to fraudulently interface with Class members, their banks and with third parties about the unlawful and recurring nature of the Pharmacy Defendants' illegal

scheme, and their identity, during the course of addressing chargebacks and other complaints arising from the Pharmacy Defendants illegal transactions, (5) to refrain from reporting the Pharmacy Defendants' activities within the Visa network, other card network operators, and other proper authorities; and (6) to remit funds to the Pharmacy Defendants.

The Underlying RICO Predicate Acts

80. 18 U.S.C. §1029 Unlawful Use of Access Devices -- The Defendants knowingly and intentionally obtained access to a number of "access devices" as that term is defined in 18 U.S.C. § 1029(e)(1), including: (1) compromised, botnet computers used to transmit spam or host pharmacy websites, (2) Project Honey Pot email addresses to which spam was transmitted; (3) the dedicated websites hosting Project Honey Pot honeypots; (3) John Doe and Class member credit card account numbers, bank information, online banking credentials, email addresses, physical addresses and IP addresses. Each of these types of information constitute "access devices" as that term is defined in 18 U.S.C. § 1029(e)(1). Those access devices were obtained by the Defendants with intent to defraud, as alleged in paragraphs 40 through 56. They were, therefore, "unauthorized access devices" as that phrase is defined in 18 U.S.C. § 1029(e)(3). The Defendants, individually and collectively, knowingly and with intent to defraud, possessed, trafficked in and used millions of unauthorized access devices during a multi-year period, and by such conduct, obtained hundreds of millions of dollars. The conduct of the Defendants described herein constituted multiple violations of 18 U.S.C. § 1029(a)(2) and (a)(3), which constitute predicate offenses for purposes of 18 U.S.C. § 1962(c). The Defendants conspired with each other and unnamed persons to commit the offenses alleged above, in violation of 18 U.S.C. § 1029(b)(2), which conspiracies are predicate offenses for purposes of 18 U.S.C. § 1962(c).

81. 18 U.S.C. § 1344 Bank Fraud -- The conduct of the Defendants as described in this complaint constituted the execution of a scheme and artifice to obtain, by means of fraudulent pretenses, representations and promises, (1) credit and debit card numbers and related card information owned by, or under the custody or control of, the financial institutions used by John Doe and the consumer members of the Class, (2) money and funds owned by, or under the custody or control of the financial institutions used by John Doe and the consumer members of the Class, and (3) moneys, fund, credits, assets or other property owned by Visa USA, Visa International or other Visa entities, other card networks, or the financial institutions that are members of Visa or other card networks. The scheme and artifice adversely affected a vast universe of persons throughout the United States, including Project Honey Pot and other email service providers receiving spam similar to that transmitted to Project Honey Pot, and banks throughout the United States providing credit card accounts to John Doe and the Class members. When Class members complained to their bank, those banks were forced to expend resources to initiate an investigation and reverse the transaction if possible. In some instances, these issuing banks covered the loss for the consumer Class member because the time period for disputing the charge with the merchant bank had expired. In addition, these banks incurred costs in closing the credit card number and issuing a new card number and physical card to the consumer Class member. These banks, and the consumer Class members, continue to incur losses as they deal with the Pharmacy Defendants' phishing and spear phishing attacks on the consumer Class members' bank account credentials. Project Honey Pot has incurred costs in receiving, processing, storing and analyzing spam messages advertising the websites used by the Defendants to consummate their bank fraud. All of these losses have occurred in violation of 18 U.S.C. § 1344, which is a predicate offense for purposes of 18 U.S.C. § 1962(c).

82. 18 U.S.C. § 1341 Mail Fraud -- The Defendants sent through and received from the United States mails materials as part of the scheme and artifice to defraud and obtain money for themselves by means of false and fraudulent pretenses, promises and representations described in this complaint. Such use of the mails included: (1) their shipment of counterfeit medications to the Class members; (2) their receipt of stolen consumer goods from merchants, where the goods were purchased using stolen credit card information or information obtained from the Class members making purchase at one of the pharmacy websites; (3) communications with and payments to: Visa, other card networks, other financial institutions, vendors, suppliers, merchants and other third parties concerning the Pharmacy Defendants, the transactions initiated on behalf of the Pharmacy Defendants, the underlying scheme, the bank's role in that scheme and other subjects. The conduct described herein constituted multiple violations of 18 U.S.C. § 1341, which is a predicate offense for purposes of 18 U.S.C. § 1962(c).

83. 18 U.S.C. § 1343 Wire Fraud -- The Defendants sent and received material by interstate and foreign wire as part of the scheme and artifice to defraud and obtain money for themselves by means of false and fraudulent pretenses, promises and representations described in this complaint. Such use of interstate and foreign wires included by way of example: (1) their operation and advertising of telephone numbers as customer service contact points; (2) their transmission of spam emails through compromised botnet computers to Project Honey Pot advertising their pharmacy websites; (3) their transmission of spam emails, creation and presentation of paid advertisements, and submissions to search engines of their online pharmacy web pages; (4) their use of Internet access in violation of access providers' terms of service to harvest email addresses from Project Honey Pot and to host their online pharmacy web pages; (5) their telephone calls and emails to Class members for purposes of extorting funds

from the Class members by posing as law enforcement agents; (6) wire transfers of funds received by the Merchant Bank Defendants to bank accounts controlled by the Pharmacy Defendants; (7) online purchases of goods and services essential to their online pharmacy business (such as domain names, email hosting, telephone services, website hosting, and physical mail delivery services), using false information including stolen credit cards or credit cards obtained from the Class members and used without their authorization. The conduct described herein constituted multiple violations of 18 U.S.C. § 1343, which is a predicate offense for purposes of 18 U.S.C. § 1962(c).

84. Dealing in Controlled Substances -- The Defendants dealt in controlled substances or listed chemicals (as defined in section 102 of the Controlled Substances Act), which is chargeable under state law and punishable by imprisonment for more than one year. The conduct constituted multiple violations of state and federal law, and is a predicate offense for purposes of 18 U.S.C. § 1962(c).

85. Extortion -- The Defendants engaged in acts and threats to extort funds from Class members, arising from the Class members' purchase of certain medications, including controlled substances or medications held out by the Defendants to be controlled substances, which is chargeable under state law and punishable by imprisonment for more than one year. Such conduct constitutes multiple violations of state law, which is a predicate offense for purposes of 18 U.S.C. § 1962(c).

86. 18 U.S.C. § 2318 Trafficking in Counterfeit Computer Software -- The Defendants engaged in acts that constitute trafficking in counterfeit computer programs or computer program documentation or packaging. Such conduct constitutes multiple violations of 18 U.S.C. § 2318, which is a predicate offense for purposes of 18 U.S.C. § 1962(c).

87. 18 U.S.C. § 2320 Trafficking in Counterfeit Marks -- The Defendants engaged in acts that constitute trafficking in goods bearing counterfeit marks. Such conduct constitutes multiple violations of 18 U.S.C. § 2320, which is a predicate offense for purposes of 18 U.S.C. § 1962(c).

88. The unlawful conduct alleged above by the Defendants injured thousands of victims, was open ended, was intended to continue indefinitely, and on information and belief is continuing at the present time.

Alternative Allegations of RICO Violations by the Defendants

89. Plaintiffs specifically re-allege that the Defendants are persons as defined in 18 U.S.C. § 1962(3).

90. In the alternative, the enterprise was an enterprise-in-fact under 18 U.S.C. § 1962(4) consisting of two or more of the following: Chernuk, Livshits, the named Merchant Banks, and other unnamed Pharmacy Defendants and unnamed Merchant Bank Defendants.

91. The enterprise-in-fact identified in the alternative above maintained substantial common management and employees and maintained substantially the same mode of operation over an extended period and continuing to the present.

92. The Defendants participated in the conduct of the affairs of the enterprise-in-fact through a "pattern of racketeering activity" as that phrase is defined in 18 U.S.C. § 1961(5).

93. Plaintiffs specifically incorporate and re-allege paragraphs 40-57 and paragraphs 73 through 87 above.

94. The unlawful conduct alleged above through the enterprise-in-fact injured thousands of victims, was open-ended, was intended to continue for an indefinite period, and on information and belief continues to the present.

COUNT III
Violation of the Federal RICO Act (Conspiracy under 18 U.S.C. § 1962(d) et seq.)
By All Plaintiffs Against the Merchant Bank Defendants

95. Plaintiffs Project Honey Pot and John Doe, on behalf of himself and the Class, repeat and re-allege the allegations in paragraphs 1 through 66 of this Complaint.

96. With knowledge of the Pharmacy Defendants' deceptive, fraudulent and unlawful conduct as alleged herein, the Merchant Bank Defendants conspired with the Pharmacy Defendants or one or more of them, to violate 18 U.S.C. § 1962(c), in violation of 18 U.S.C. § 1962(d).

97. Each of the Merchant Bank Defendants joined the conspiracy at least as early as the first time each bank accepted one or more of the Pharmacy Defendants as a merchant for purposes of processing credit card transactions.

98. For the reasons stated above in paragraphs 76 through 78, the Merchant Bank Defendants were on notice of and knew of the unlawful scheme being perpetrated by the Pharmacy Defendants as alleged herein, but nonetheless conspired and agreed to facilitate the scheme, and committed acts in furtherance of that scheme, in violation of 18 U.S.C. § 1962(d), by continuing: (1) to process credit card transactions, (2) to open new merchant accounts for the Pharmacy Defendants; (3) to collect funds from transactions tied to merchant accounts controlled by the Pharmacy Defendants, (4) to fraudulently interface with Class members, their banks and with third parties about the unlawful and recurring nature of the Pharmacy Defendants' illegal scheme, and their identity, during the course of addressing chargebacks and other complaints

arising from the Pharmacy Defendants illegal transactions, (5) to refrain from reporting the Pharmacy Defendants' activities to Visa, other card network operators, and other proper authorities; and (6) to remit funds to the Pharmacy Defendants.

99. Plaintiffs Project Honey Pot, John Doe and the Class members were the intended targets of the scheme that was facilitated by the knowing and purposeful involvement of the Merchant Bank Defendants. The financial harms suffered by Plaintiffs and the members of the Class were by reason of said conduct and were the reasonably foreseeable consequences of such conduct.

COUNT IV
Violation of the Federal CAN-SPAM Act (15 U.S.C. § 7701 et seq.)
By Project Honey Pot Against All Defendants

100. Plaintiff Project Honey Pot repeats and re-alleges the allegations in paragraphs 1 through 66 of this Complaint.

101. Defendants initiated the transmission, to a protected computer, of a commercial electronic mail message that contained, or was accompanied by, header information that was materially false or materially misleading, in violation of 15 U.S.C. § 7704(a)(1).

102. In a pattern or practice, Defendants initiated the transmission to a protected computer of a commercial electronic mail message that did not contain a functioning return electronic mail address or other Internet-based mechanism, clearly and conspicuously displayed, that a recipient could use to submit, in a manner specified in the message, a reply electronic mail message or other form of Internet-based communication requesting not to receive future commercial electronic mail messages from that sender at the electronic mail address where the message was received, in violation of 15 U.S.C. § 7704(a)(3).

103. In a pattern or practice, Defendants initiated the transmission of a commercial electronic mail message to a protected computer and failed to provide: (i) clear and conspicuous identification that the message was an advertisement or solicitation; (ii) clear and conspicuous notice that the recipient could decline to receive further commercial electronic mail messages from the sender; and (iii) a valid physical postal address of the sender, in violation of 15 U.S.C. § 7704(a)(5).

104. Plaintiff Project Honey Pot is an Internet access service adversely affected by the above violations, and is entitled to an injunction barring further violations, statutory damages of $100 for every attempted transmission of a spam message that contains false or misleading transmission information, statutory damages of $25 for every attempted transmission of a spam message that otherwise fails to comply with the Federal CAN-SPAM Act, treble damages resulting from Defendants' use of email harvesters and dictionary attacks to facilitate their violations of the CAN-SPAM Act, and attorney fees and costs, as authorized by 15 U.S.C. § 7706(g).

COUNT V
Violation of Virginia's Anti-Spam Statute (18 Va. Code § 18.2-152.3:1 et seq.)
By Plaintiff Project Honey Pot Against All Defendants

105. Plaintiff Project Honey Pot repeats and re-alleges the allegations in paragraphs 1 through 66 of this Complaint.

106. Defendants used a computer or computer network with the intent to falsify or forge electronic mail transmission information or other routing information in any manner in connection with the transmission of bulk electronic mail through or into the computer network of an electronic mail service provider or its subscribers.

107. Defendants' transmissions were in contravention of the authority granted by or in violation of the policies set by Plaintiff. Defendants had knowledge of the authority or policies of those email service providers, or the authority or policies were available on Project Honey Pot's website.

108. As a result of Defendants' actions, Plaintiff Project Honey Pot has suffered injury, and is entitled to an injunction, and to recover actual damages, or in lieu thereof $1 for each and every unsolicited bulk electronic mail message transmitted in violation of the statute, or $25,000 per day any offending message was transmitted, plus attorneys' fees and costs of suit.

COUNT VI
Common Law Conspiracy
By All Plaintiffs Against All Defendants

109. Plaintiffs Project Honey Pot and John Doe, on behalf of himself and the Class, repeat and re-allege the allegations in paragraphs 1 through 66 of this Complaint.

110. The Defendants have conspired and combined with one another and third parties to operate illegal online pharmacies and engage in other illegal activities alleged in this complaint. Defendants' acts of conspiracy have been undertaken intentionally, with malice, oppression and fraud, justifying the imposition of punitive damages in amount sufficient to punish Defendants and deter Defendants and others from engaging in similar conduct.

111. Defendants' acts have caused injury to Project Honey Pot, John Doe and the Class members.

112. As a result of Defendants' conspiracy, the Plaintiffs have suffered and will continue to suffer irreparable injury. Unless enjoined by this Court, Defendants will continue these acts, thereby causing Plaintiffs continuing and irreparable damage.

COUNT VII
(Negligence, Negligent Enablement, Negligent Hiring and Retention)
By All Plaintiffs Against the Merchant Bank Defendants

113. Plaintiffs Project Honey Pot and John Doe, on behalf of himself and the Class members, repeat and re-allege the allegations in paragraphs 1 through 66 of this Complaint.

114. The Merchant Bank Defendants have negligently provided critical enabling services to the Pharmacy Defendants, whom they knew or should have known were using these services to further their illegal schemes, and retained the Pharmacy Defendants as merchants, and negligently hired and retained merchant account brokers, independent sales organizations, processors and Internet Payment Service Providers to procure, manage, process and supervise the Pharmacy Defendants' merchant account activities. The Merchant Bank Defendants had a duty to the Plaintiffs and each of them to act in a non-negligent manner because it was foreseeable that the actions of the Pharmacy Defendants, merchant account brokers, independent sales organizations and Internet Payment Service Providers would harm the Plaintiffs.

115. As a result of the Merchant Banks' negligence, Plaintiffs and each of them have suffered and will continue to suffer irreparable injury and pecuniary damages. Unless enjoined by this Court, the Merchant Bank Defendants will continue these acts thereby causing the Plaintiffs continuing and irreparable damage.

116. The Merchant Bank Defendants' practice of negligently enabling, hiring and retaining the Pharmacy Defendants, and merchant account brokers, independent sales organizations and processors and Internet Payment Service Providers to generate sales through their illegal online pharmacy scheme has been undertaken with malice, oppression and fraud,

justifying the imposition of punitive damages in an amount sufficient to punish the Merchant Bank Defendants and deter them and others from engaging in similar conduct.

COUNT VIII
Unjust Enrichment
By All Plaintiffs Against Merchant Bank Defendants

117. Plaintiffs Project Honey Pot and John Doe, on behalf of himself and the Class members, repeat and re-allege the allegations in paragraphs 1 through 66 of this Complaint.

118. By their actions alleged herein, the Merchant Bank Defendants have knowingly obtained, conferred, or retained benefits acquired at the expense of the Plaintiffs and each of them. The Merchant Bank Defendants' knowing acquisition of these benefits has occurred under circumstances that render it inequitable for them to retain the benefits without paying for their value.

119. As a result of their unjust enrichment, the Merchant Bank Defendants should be ordered to compensate the Plaintiffs, and each of them, for the value of the benefits unlawfully acquired by the Merchant Bank Defendants, and ordered to disgorge all profits derived from the illegal schemes alleged herein. A constructive trust should also be imposed in favor of the Plaintiffs on all moneys received by or due the Merchant Bank Defendants and on all profits generated by Defendants' illegal activities as a result of their illegal scheme, and on all real property, motor vehicles, cash, demand deposit bank accounts and other personal property purchased with moneys by the Merchant Bank Defendants as a result of their illegal activities.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs demand this case be tried to a jury, and request entry of judgment in their favor and against Defendants:

1. Granting preliminary and permanent injunctive relief against Defendants, and all those in privity or acting in concert with Defendants, enjoining them from directly or indirectly violating the terms of the Federal False Marking Act, the Federal RICO Act, and the Federal CAN-SPAM Act or the terms of the Virginia anti-spam statute;

2. Awarding Plaintiffs compensatory and punitive damages in an amount to be proven at trial;

3. Awarding Plaintiffs attorneys' fees and costs associated with prosecuting this action; and

4. Granting Plaintiffs such other or additional relief as this Court deems just and proper under the circumstances.

Dated: July 12, 2011

Respectfully submitted,

/s/

Jon L. Praed
VSB #40678
Attorney for Plaintiffs,
Project Honey Pot, John Doe, on behalf of himself and all others similarly situated
Internet Law Group
4121 Wilson Boulevard, Suite 101
Arlington, Virginia 22203
Phone: (703) 243-8100 x223
Fax: (703) 522-1527
jon.praed@i-lawgroup.com